What is claimed is:

[Claim 1] 1. A method for accessing discrete data comprising:

(a) transmitting a write command to a memory;

(b) according to a data format of a file that is to be written into the memory, determining whether each data following a header of the file needs to be encrypted, and transmitting the file header and each data following the file header to a logic unit;

(c) turning on the logic unit for encrypting the data determined to be encrypted in step (b) and writing the encrypted data into the memory;

(d) turning off the logic unit for writing the data determined not to be encrypted in step (b) into the memory directly; and

(e) sending a first response signal from the memory when the writing of the file is finished.

[Claim 2] 2. The method of claim 1 wherein the data following the file header comprises one or a plurality of frames, in which each frame comprises a header, a data block and a residual block, wherein the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the residual block of each frame are determined not to be encrypted, and the data block of each frame is determined to be encrypted in step (b).

[Claim 3] 3. The method of claim 1 wherein the first response signal is a writing succeeded signal.

[Claim 4] 4. The method of claim 1 transmitting the file header and each data following the file header from a plurality of buffers in turn to the logic unit in step (b).

[Claim 5] 5. The method of claim 1 wherein step (c) further comprises changing the data format from little-endian to big-endian, or changing the data format from big-endian to little-endian before writing the encrypted data into the memory.

[Claim 6] 6. The method of claim 1 wherein the encryption algorithm is performed according to the specification of content protection for recordable media (CPRM).

[Claim 7] 7. The method of claim 1 further comprising:

(f) transmitting a read command to the memory;

(g) according to a data format recorded in a header of a file that is to be read from the memory, determining whether each data following the file header needs to be decrypted, and transmitting the file header and each data following the file header to a logic unit;

(h) turning on the logic unit for decrypting the data determined to be decrypted in step (g) and writing the decrypted data into a buffer;

(i) turning off the logic unit for writing the data determined not to be decrypted in step (g) into the buffer directly; and

(j) sending a second response signal from the memory when the writing of the file is finished.

[Claim 8] 8. The method of claim 7 wherein the data following the file header comprises one or a plurality of frames, wherein each frame comprises a header, a data block and a residual block, wherein the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the residual block of each frame are determined not to be decrypted, and the data block of each frame is determined to be decrypted in step (g).

[Claim 9] 9. The method of claim 7 wherein the second response signal is a reading succeeded signal.

[Claim 10] 10. The method of claim 7 wherein the logic unit writes the data into a plurality of buffers in turn.

[Claim 11] 11. The method of claim 7 wherein step (h) further comprises changing the data format from little-endian to big-endian, or changing the data format from big-endian to little-endian before writing the decrypted data into the buffer.

[Claim 12] 12. The method of claim 7 wherein the decryption algorithm is performed according to the specification of content protection for recordable media.

[Claim 13] 13. The method of claim 1 wherein the memory is a flash memory.

[Claim 14] 14. The method of claim 1 wherein the memory is a secure digital (SD) card.

[Claim 15] 15. The method of claim 1 wherein the memory is a digital video disk (DVD).

[Claim 16] 16. The method of claim 1 wherein the file is an audio file.

[Claim 17] 17. The method of claim 1 wherein the file is a video file.

[Claim 18] 18. A method for accessing discrete data comprising:

(a) transmitting a read command to a memory;

(b) according to a data format recorded in a header of the file that is to be read from the memory, determining whether each data following the file header needs to be decrypted, and transmitting the file header and each data following the file header to a logic unit;

(c) turning on the logic unit for decrypting the data determined to be decrypted in step (b) and writing the decrypted data into a buffer;

(d) turning off the logic unit for writing the data determined not to be decrypted in step (b) into the buffer directly; and

(e) sending a first response signal from the memory when the writing of the file is finished.

[Claim 19] 19. The method of claim 18 wherein the data following the file header comprises one or a plurality of frames, wherein each frame comprises a header, a data block and a residual block, wherein the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the

residual block of each frame are determined not to be decrypted, and the data block of each frame is determined to be decrypted in step (b).

[Claim 20] 20. The method of claim 18 wherein the first response signal is a reading succeeded signal.

[Claim 21] 21. The method of claim 18 wherein the logic unit writes the data into a plurality of buffers in turn.

[Claim 22] 22. The method of claim 18 wherein step (c) further comprises changing the data format from little-endian to big-endian, or changing the data format from big-endian to little-endian before writing the decrypted data into the buffer.

[Claim 23] 23. The method of claim 18 wherein the memory is a flash memory.

[Claim 24] 24. The method of claim 18 wherein the memory is a secure digital (SD) card.

[Claim 25] 25. The method of claim 18 wherein the memory is a digital video disk (DVD).

[Claim 26] 26. The method of claim 18 wherein the method of decryption is performed according to the decryption algorithm of the specification of content protection for recordable media.

[Claim 27] 27. The method of claim 18 wherein the file is an audio file.

[Claim 28] 28. The method of claim 18 wherein the file is a video file.

[Claim 29] 29. A discrete data accessing system comprising:

a memory for storing data;

a first logic unit electrically connected to the memory for encrypting input data according to a predetermined encryption algorithm, writing the encrypted data into the memory, or writing input data into the memory directly; and

a second logic unit electrically connected to the first logic unit for determining whether each data following a header of a file that is to be written into the memory needs to be encrypted according to a data format of the file in order to decide whether to turn on the first logic unit for encrypting the input data and writing the encrypted data into the memory, or to turn off the first logic unit for writing the input data into the memory directly.

[Claim 30] 30. The system of claim 29 wherein the data following the file header comprises one or a plurality of frames, wherein each frame comprises a header, a data block and a residual block, in which the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the residual block of each frame are determined not to be encrypted, and the data block of each frame is determined to be encrypted by the second logic unit.

[Claim 31] 31. The system of claim 29 wherein the first logic unit is further capable of changing the data format from little-endian to big-endian, or

changing the data format from big-endian to little-endian before writing the encrypted data into the memory.

[Claim 32] 32. The system of claim 29 wherein the encryption algorithm is performed according to the specification of content protection for recordable media.

[Claim 33] 33. The system of claim 29 further comprising a buffer wherein the first logic unit is further capable of decrypting input data according to a predetermined decryption algorithm and writing the decrypted data into the buffer, or writing the input data into the buffer directly, and the second logic unit is further capable of determining whether each data following a header of a file that is to be read from the memory needs to be decrypted according to a data format recorded in the file header in order to decide whether to turn on the decryption function of the first logic unit for decrypting the input data and writing the decrypted data into the buffer, or to turn off the decryption function of the first logic unit for writing the input data into the buffer directly.

[Claim 34] 34. The system of claim 33 wherein the data following the file header comprises one or a plurality of frames, in which each frame comprises a header, a data block and a residual block, wherein the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the residual block of each frame are determined not to be decrypted, and the data block of each frame is determined to be decrypted by the second logic unit.

[Claim 35] 35. The system of claim 33 wherein the first logic unit is further capable of changing the data format from little-endian to big-endian, or

changing the data format from big-endian to little-endian before writing the decrypted data into the buffer.

[Claim 36] 36. The system of claim 33 wherein the decryption algorithm is performed according to the specification of content protection for recordable media.

[Claim 37] 37. The system of claim 29 further comprising a buffer and a third logic unit wherein the third logic unit is capable of decrypting input data according to a predetermined decryption algorithm and writing the decrypted data into the buffer, or writing the input data into the buffer directly, and the second logic unit is further capable of determining whether each data following a header of a file that is to be read from the memory needs to be decrypted according to a data format recorded in the file header in order to decide whether to turn on the decryption function of the third logic unit for decrypting the input data and writing the decrypted data into the buffer, or to turn off the decryption function of the third logic unit for writing the input data into the buffer directly.

[Claim 38] 38. The system of claim 37 wherein the data following the file header comprises one or a plurality of frames, in which each frame comprises a header, a data block and a residual block, wherein the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the residual block of each frame are determined not to be decrypted, and the data block of each frame is determined to be decrypted by the second logic unit.

[Claim 39] 39. The system of claim 37 wherein the third logic unit is further capable of changing the data format from little-endian to big-endian, or

changing the data format from big-endian to little-endian before writing the decrypted data into the buffer.

[Claim 40] 40. The system of claim 37 wherein the decryption algorithm is performed according to the specification of content protection for recordable media.

[Claim 41] 41. The system of claim 29 wherein the memory is a flash memory.

[Claim 42] 42. The system of claim 29 wherein the memory is a secure digital (SD) card.

[Claim 43] 43. The system of claim 29 wherein the memory is a digital video disk (DVD).

[Claim 44] 44. The system of claim 29 wherein the file is an audio file.

[Claim 45] 45. The system of claim 29 wherein the file is a video file.

[Claim 46] 46. A discrete data accessing system comprising:

a memory for storing data;

a buffer for storing data;

a first logic unit electrically connected to the buffer for decrypting input data according to a predetermined decryption algorithm and writing the decrypted data into the buffer, or writing the input data into the buffer directly; and

a second logic unit electrically connected to the first logic unit for determining whether each data following a header of a file that is to be read from the memory needs to be decrypted according to a data format recorded in the file header in order to decide whether to turn on the decryption function of the first logic unit for decrypting the input data from the memory and writing the decrypted data into the buffer, or to turn off the decryption function of the first logic unit for writing the input data from the memory into the buffer directly.

[Claim 47] 47. The system of claim 46 wherein the data following the file header comprises one or a plurality of frames, in which each frame comprises a header, a data block and a residual block, wherein the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the residual block of each frame are determined not to be decrypted, and the data block of each frame is determined to be decrypted by the second logic unit.

[Claim 48] 48. The system of claim 46 wherein the first logic unit is further capable of changing the data format from little-endian to big-endian, or changing the data format from big-endian to little-endian before writing the decrypted data into the buffer.

[Claim 49] 49. The system of claim 46 wherein the decryption algorithm is performed according to the specification of content protection for recordable media.

[Claim 50] 50. The system of claim 46 wherein the memory is a flash memory.

[Claim 51] 51. The system of claim 46 wherein the memory is a secure digital (SD) card.

[Claim 52] 52. The system of claim 46 wherein the memory is a digital video disk (DVD).

[Claim 53] 53. The system of claim 46 wherein the file is an audio file.

[Claim 54] 54. The system of claim 46 wherein the file is a video file.